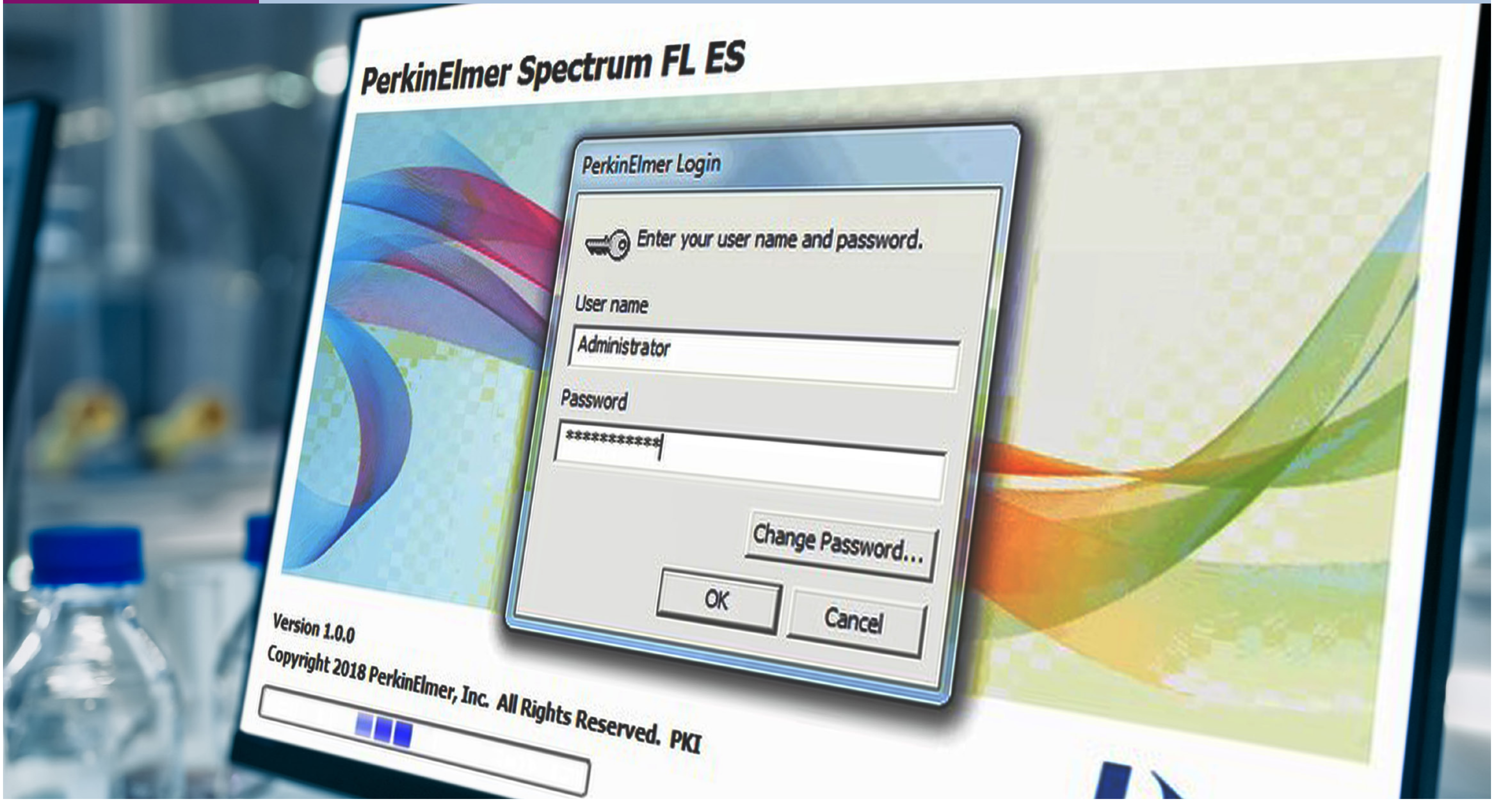
WHITE PAPER

Data Integrity – Spectrum FL Enhanced Security (ES) Software for Fluorescence Spectroscopy



PerkinElmer Spectrum FL ES

PerkinElmer Login

Enter your user name and password.

User name: Administrator

Password: ***********

Version 1.0.0

Copyright 2018 PerkinElmer, Inc. All Rights Reserved. PKI

Introduction

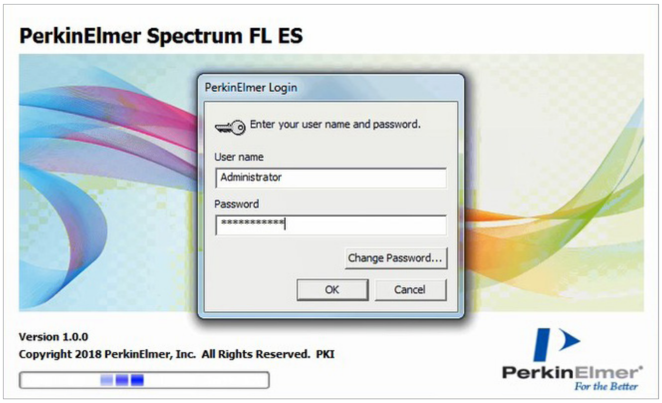
The FDA defines data integrity as "completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)".[1] ALCOA itself has evolved to ALCOA Plus, which incorporates two of the fundamental definition terms as stated by the FDA; complete, consistent, enduring and available.[2] Compliance with 21 CFR Part 11 is mandatory for pharmaceutical companies and their suppliers to sell products into the United States, and also applies to other related industries.

PerkinElmer's Spectrum™ FL Enhanced Security (ES) software platform for fluorescence spectroscopy provides structural requirements and features to match the specific needs for ensuring data integrity. It affords the system owner the ability to comply with regulations and incorporate features into the validation plan to exhibit compliance. The purpose of this document is to demonstrate how Spectrum FL ES meets the technical requirements for 21 CFR Part 11.

Spectrum FL ES

Spectrum FL ES, based on PerkinElmer's well-established Spectrum 10 ES software, provides tightly controlled setup, collection and reporting of fluorescence data to meet the technical demands of 21 CFR Part 11 compliance (Figures 1 and 2). Spectrum FL ES is compatible with the FL 6500™ and FL 8500™ fluorescence instruments and benefits from an easy-to-use workflow-oriented interface for quick training of analysts. Most functions within Spectrum FL are identical in standard (STD) and ES versions. However, the main differences are related to:

- Logins
- Permissions
- Electronic signatures
- Protection of records
- Working with audit trails



PerkinElmer Spectrum FL ES

PerkinElmer Login

Enter your user name and password.

User name: Administrator

Password: ***********

Version 1.0.0

Copyright 2018 PerkinElmer, Inc. All Rights Reserved. PKI

Figure 1. Login window for Spectrum FL ES software.

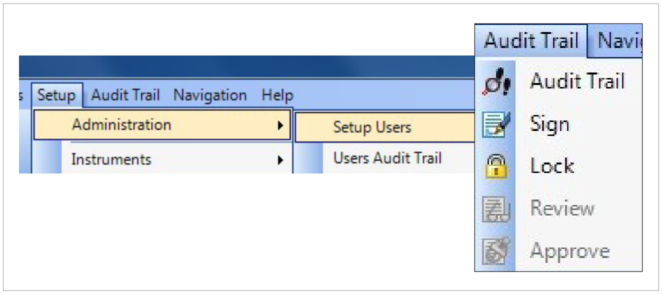


Figure 2. Enhanced security features are shown on the tool bar in Spectrum FL.

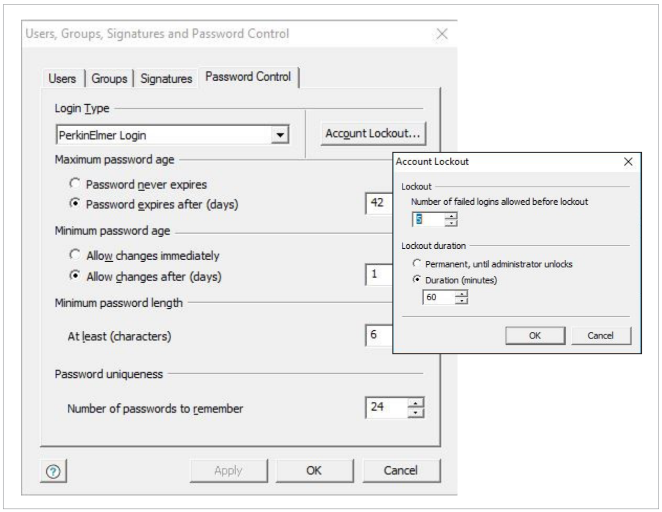
Software Logins

Unique user names and passwords are required for all authorized users to access Spectrum FL ES software and cannot be reassigned. The instrument Service Mode is also under password control. Users can be setup by the Administrator in the software (Figure 3).

Two password login modes are available:

- PerkinElmer login ➞ logins (user name and password) are created for each Spectrum User and remain unique within the system, even after a user has left the company
- Windows® login ➞ login is controlled by the login to the Windows® OS, meaning only one password to remember

For complete technical compliance with 21 CFR Part 11, the login security includes administrator-definable features such as password expiration and failed login detection and lockout. All access or attempted access to the system is logged in an audit trail. Users are limited to a specified number of unsuccessful login attempts. If the administrator-defined number of unsuccessful PerkinElmer logins is reached, that user is locked out for a certain period (defined by the administrator) or once they have been unlocked by the administrator. The Spectrum FL ES Administrator can allocate a new temporary password, which the user is forced to change on its first-time use (i.e. their next login). Due to the high degree of security in Spectrum FL ES, it is highly recommended that more than one Administrator be created in case one of the Administrators is absent or forgets their password. The software has no 'backdoor' to the security system. If a user is locked out whilst using the Windows login, the company IT administrator will need to unlock their account and/or provide them with a temporary password.



Users, Groups, Signatures and Password Control

Login Type: PerkinElmer Login

Maximum password age
○ Password never expires
● Password expires after (days) 42

Minimum password age
○ Allow changes immediately
● Allow changes after (days) 1

Minimum password length
At least (characters) 6

Password uniqueness
Number of passwords to remember 24

Account Lockout

Lockout
Number of failed logins allowed before lockout 5

Lockout duration
○ Permanent, until administrator unlocks
● Duration (minutes) 60

Figure 3. Setup of logins and password control (left) and account lockout (right).

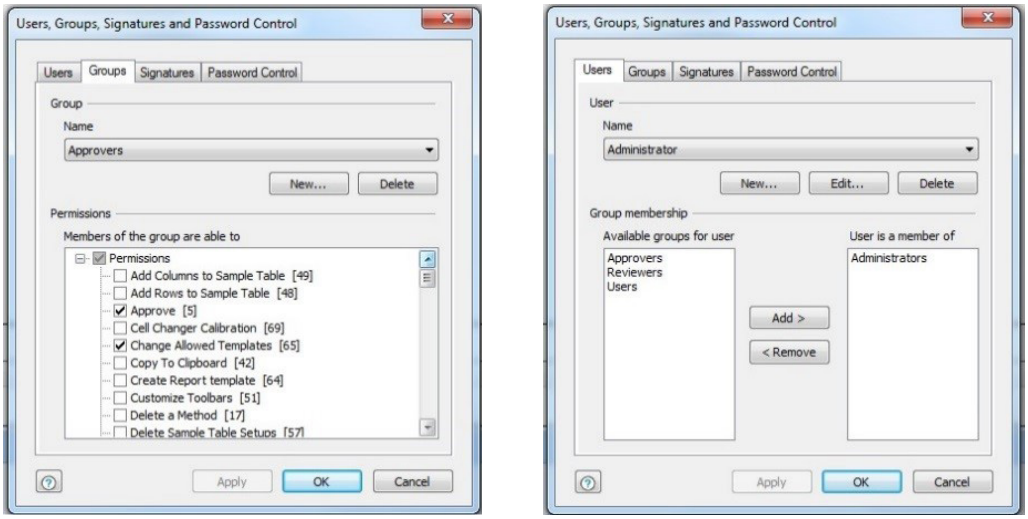
Permissions for Users and User Groups

Spectrum FL ES enforces authority checks using authorization groups. Each group has its software access rights defined by the selection of permissions. Individual users are assigned to one or more of these pre-defined groups. At installation, the software has a default set of authorization groups.

Default groups include:

- **Administrators** – The permissions for the 'Administrators' group cannot be changed. Only members of the Administrators group can perform Administration tasks – setup users, groups and passwords.
- **Users** – By default, members of the 'Users' group can perform all functions in the software, except those associated with Administrators and Return Workspace, Review, and Approve.
- **Reviewers** – Members of the 'Reviewers' group are intended to act as reviewers of changes, made by other users, requiring an electronic signature. Members of the Reviewers group cannot set up other users. (Default permissions: Review, Return Workspace, Import/export Sample Table Setups, Import/Export Instrument Setup, and Setup Equations only).
- **Approvers** – Members of the Approvers group are intended to act as approvers of changes, made by other users, requiring an electronic signature. Members of the Approvers group cannot set up other users. (Default permissions: Approve, Return Workspace, Import/Export Sample Table Setups, Import/Export Instrument Setup, and Setup Equations only).

Only Spectrum FL ES Administrators can alter the permissions of the accessible functions for these groups, add new groups, maintain the system, and allocate areas of access to individual users. The groups to which a user belongs can be toggled and define the areas of software they are permitted access to (Figure 4). This allows the application to be customized to the laboratory's most effective workflow according to their specific analytical requirements. Spectrum FL ES allows individual methods to be signed for, reviewed, and approved (Figure 5).



Name: Approvers

- ☑ Permissions
  - □ Add Columns to Sample Table [49]
  - □ Add Rows to Sample Table [48]
  - ☑ Approve [5]
  - □ Cell Changer Calibration [69]
  - ☑ Change Allowed Templates [65]
  - □ Copy To Clipboard [42]
  - □ Create Report template [64]
  - □ Customize Toolbars [51]
  - □ Delete a Method [17]
  - □ Delete Sample Table Setups [57]

Name: Administrator

Available groups for user: Approvers, Reviewers, Users

User is a member of: Administrators

Figure 4. Setting up group membership (top) and group permissions (bottom).

Additionally, the Administrator can setup a default group workspace (Figure 6). This will allow an Administrator to transfer their current settings to all groups selected.

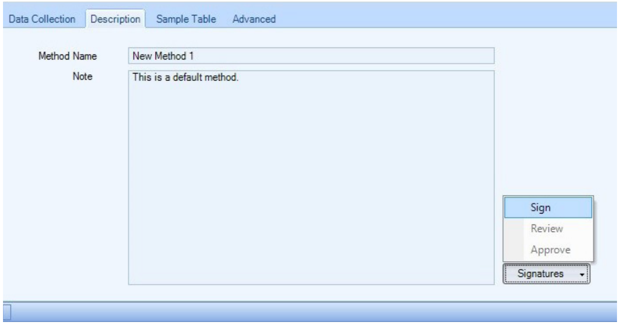
Electronic Signatures

Administrators in Spectrum FL ES can configure Signature Points for certain actions, such as data collection and outputting of results (Figure 7). Signature points can be configured individually, or the same settings can be applied to all Signature Points. Signatures can be entered on exiting, before the action (as appropriate), or by selecting 'Audit Trail' and then 'Sign'. Signatures are also added to report files.

The list of Signature Points within the software is pre-defined, and includes:

- Loading and saving instrument settings files
- Reporting on ready checks and instrument validation
- Generating reports
- Exporting data
- Deleting graphs
- Creating or making changes to equations
- Approving and reviewing items that have been signed by other users

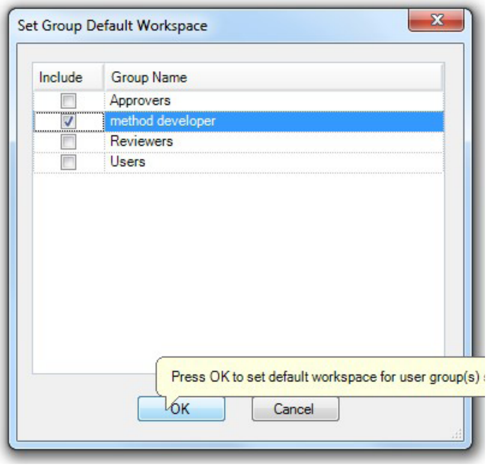
The user will not be prompted for a signature if 'Signature Required' is not selected for a signature point. The Administrator can decide whether the signature point requires a pre-defined reason and/or comment. These pre-defined reasons are displayed as a drop-down list at the time of signing. Figure 8 shows examples of available signature dialog box configurations. In the 'Comments' section, any additional information may be added. The audit trail will record the user name, date and time when the signature happened, the comment and/or pre-defined reason.



Method Name: New Method 1

Note: This is a default method.

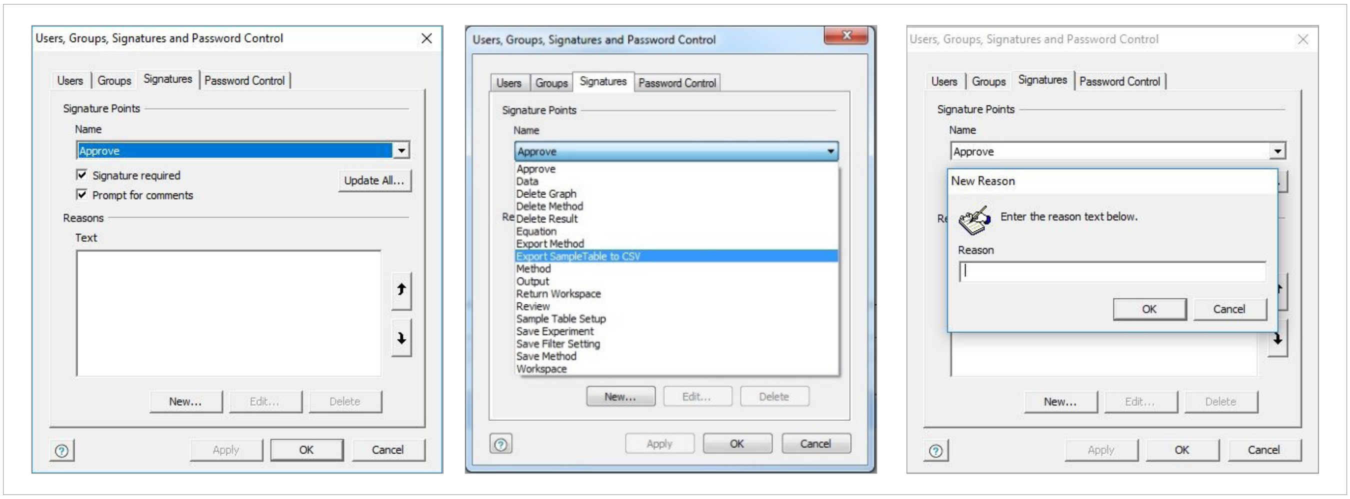
Figure 5. Setting up group workspaces.



Include	Group Name
□	Approvers
☑	method developer
□	Reviewers
□	Users

Press OK to set default workspace for user group(s)

Figure 6. Signing, reviewing and approving a method.



Users, Groups, Signatures and Password Control

Signature Points

Name: Approve

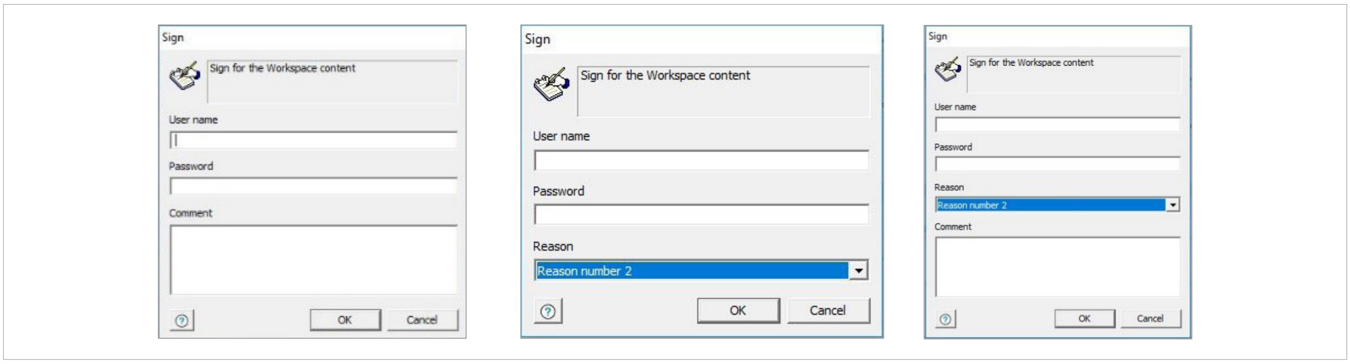
☑ Signature required

☑ Prompt for comments

New Reason

Enter the reason text below.

Figure 7. Configuring settings for individual Signature Points.



Sign

Sign for the Workspace content

Reason: Reason number 2

Figure 8. Signature dialog box configurations.

Protection of Records

Spectrum FL ES stores data in a secured SQL database to ensure complete file protection and integrity of data. Many systems use a 'flat file' approach in which spectra are saved as single files (as occurs with Spectrum STD). Utilizing flat files requires a more involved and intensive process to ensure security of results. Flat files are also limited with respect to the audit trail information they can keep. Spectrum FL ES gives operators the flexibility to use either flat file or database approaches, and this helps them with transitions from a flat file method to the preferred secured database. In addition, Spectrum FL ES has a security database which handles system security such as logins, passwords, users, groups, and electronic signature policies.

PerkinElmer secured databases are used to manage data, setups and reports. If data has not been signed for when a power failure occurs, that data can be recovered from the software and be signed for and saved. Workspaces can also be retrieved from the database to reproduce a working environment to replicate that environment at the time the workspace was saved, which includes data and settings.

The FDA is promoting pharmaceutical companies and related industries to review and approve data electronically. This can be achieved locally on a stand-alone configuration, or even remotely with a network database, using Spectrum FL ES software. Saving data on a network simplifies data backup for IT groups.

Audit Trails

Spectrum FL ES user and results/workspace audit trails are complete, consistent, and comprehensive, and it is possible to view, print and export these for inspection purposes.

Results/Workspace Audit Trail

The workspace audit trail (Figure 8) records all data, settings and actions (obtaining spectra, saving methods, fitting accessories etc.) carried out by a user in Spectrum FL ES. This audit trail also contains details of the user, the date and time stamp when the record was created, modified or deleted, the new value, the old value, and the type of modification. A Spectrum FL database has a default maximum size of 5 GB. When it reaches this size, a new database is automatically created.

The audit trail file is updated when the changes will take effect. As an example, if the instrument settings are changed, the audit trail will record this information only when the scan button is pressed. Therefore, if the instrument settings are changed, and then changed again before scanning, only the latest scan settings will be updated in the audit trail upon scanning. Any changes made to the settings which are subsequently cancelled, without being used, are not recorded.

Changes to the records will not obscure previous entries and changes which affect signed data cause a new file (spectrum file etc.) to be created, thus retaining the original. Results or data generated in the software will not be able to be removed or overwritten.

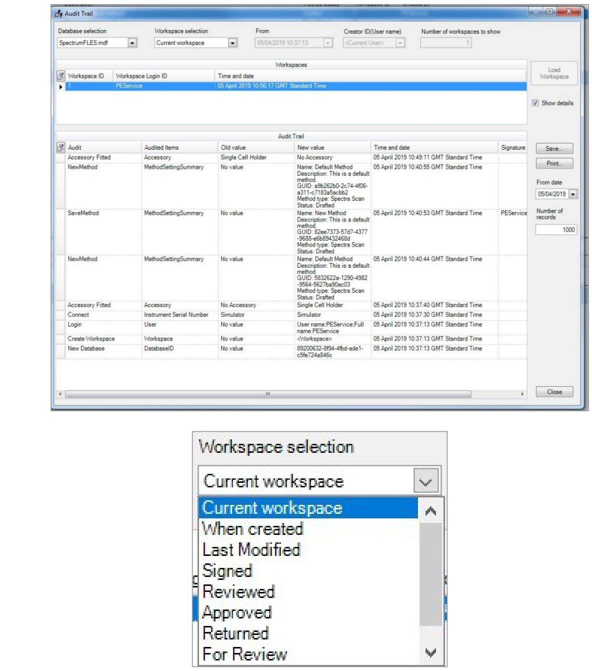
Workspaces can be retrieved to reproduce the working environment at the time the workspace was saved – including data and settings. Members of the Users group can only view workspaces they have created. However, members of the 'Administrators' group can view the Audit Trail for all workspaces (Figure 9), although they will be read-only. Members of the groups 'Reviewers' and 'Approvers' can view the Audit Trail of workspaces that have been locked by other users for review or approval.

Additionally, within the spectra files, a spectrum history is available (Figure 10). This records all sample details, the instrument settings used, any corrections applied during the scan, and all actions applied to the data after data collection. The sample history will include the user who performed these actions, which are typically of a processing nature.

Users Audit Trail and Login History

The users audit trail and login history can be viewed by members of the Administrators group only (Figure 11) and are saved in the security database. The users audit trail records all changes to security settings (users, groups, password settings) in compliance with 21 CFR Part 11. The login history details the user, their login and logout times, and the status of the login (e.g. a failed login). It also lists anomalies, such as forced logouts from software crashes. The summary tab contains a list of settings and permissions applied to the workspace and user.

Spectrum FL ES allows Administrators to view, print and export the login history and user audit trail for inspection purposes. It is only possible to clear login history and audit trail entries from the dialog that have previously been exported. If the audit trail contains additional entries since it was last exported, only those entries that have been archived will be removed if requested. If none of the entries have been archived, a warning message will be displayed upon attempt to clear the audit trail or login history (Figure 12). The dialog always records when records in the login history or audit trail have been exported and cleared.


Audit Trail

Database selection: SpectrumFLES.mdf
Workspace selection: Current workspace
From: 05/04/2019 10:37:13
Creator ID(User name): <Current User>
Number of workspaces to show: 1

Workspaces

Workspace ID	Workspace Login ID	Time and date
1	PEService	05 April 2019 10:56:17 GMT Standard Time

☑ Show details

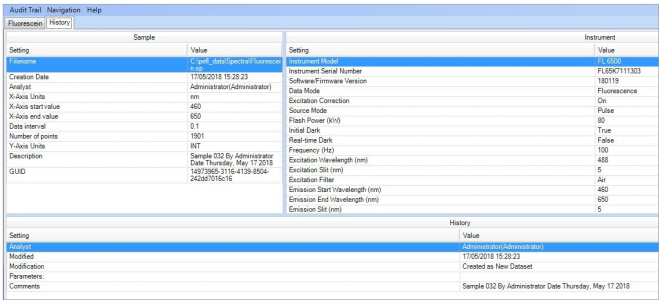
Audit Trail

Audit	Audited Items	Old value	New value	Time and date	Signature
Accessory Fitted	Accessory	Single Cell Holder	No Accessory	05 April 2019 10:49:11 GMT Standard Time	
NewMethod	MethodSettingSummary	No value	Name: Default Method Description: This is a default method. GUID: a9b262b0-2c74-4f06-a311-c7183a5acbb2 Method type: Spectra Scan Status: Drafted	05 April 2019 10:40:55 GMT Standard Time	
SaveMethod	MethodSettingSummary	No value	Name: New Method Description: This is a default method. GUID: 82ee7373-57d7-4377-9688-e6b89432468d Method type: Spectra Scan Status: Drafted	05 April 2019 10:40:53 GMT Standard Time	PEService
NewMethod	MethodSettingSummary	No value	Name: Default Method Description: This is a default method. GUID: 5832622a-1290-4982-9564-5627ba90ac03 Method type: Spectra Scan Status: Drafted	05 April 2019 10:40:44 GMT Standard Time	
Accessory Fitted	Accessory	No Accessory	Single Cell Holder	05 April 2019 10:37:40 GMT Standard Time	
Connect	Instrument Serial Number	Simulator	Simulator	05 April 2019 10:37:30 GMT Standard Time	
Login	User	No value	User name:PEService;Full name:PEService	05 April 2019 10:37:13 GMT Standard Time	
Create Workspace	Workspace	No value	<Workspace>	05 April 2019 10:37:13 GMT Standard Time	
New Database	DatabaseID	No value	89200632-8f94-4fbd-ade1-c5fe724a846c	05 April 2019 10:37:13 GMT Standard Time	

From date: 05/04/2019
Number of records: 1000

Workspace selection
Current workspace
- Current workspace
- When created
- Last Modified
- Signed
- Reviewed
- Approved
- Returned
- For Review

Figure 9. Results/workspace audit trail.


Audit Trail Navigation Help

Fluorescein | History

Sample

Setting	Value
Filename	C:\pefl_data\Spectra\Fluorescein.sp
Creation Date	17/05/2018 15:28:23
Analyst	Administrator(Administrator)
X-Axis Units	nm
X-Axis start value	460
X-Axis end value	650
Data interval	0.1
Number of points	1901
Y-Axis Units	INT
Description	Sample 032 By Administrator Date Thursday, May 17 2018
GUID	14973965-3116-4139-8504-242dd7016c16

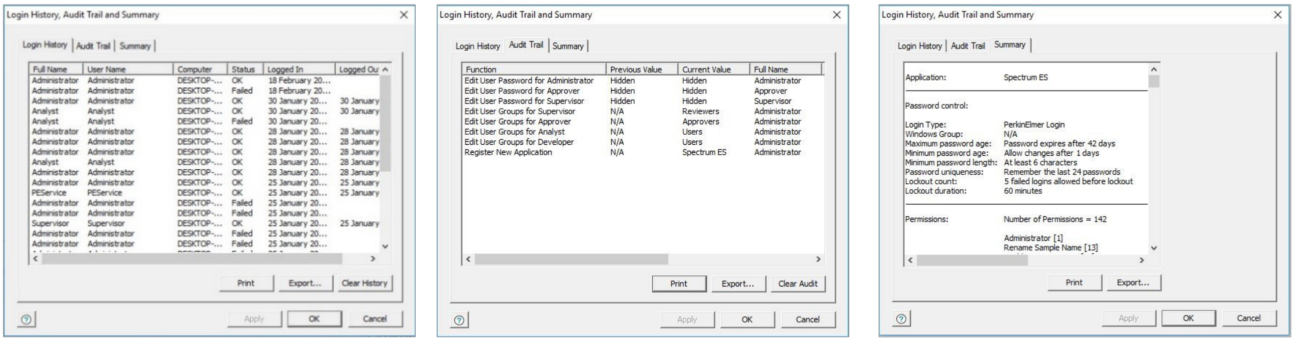
Instrument

Setting	Value
Instrument Model	FL 6500
Instrument Serial Number	FL65K7111303
Software/Firmware Version	180119
Data Mode	Fluorescence
Excitation Correction	On
Source Mode	Pulse
Flash Power (kW)	80
Initial Dark	True
Real-time Dark	False
Frequency (Hz)	100
Excitation Wavelength (nm)	488
Excitation Slit (nm)	5
Excitation Filter	Air
Emission Start Wavelength (nm)	460
Emission End Wavelength (nm)	650
Emission Slit (nm)	5

History

Setting	Value
Analyst	Administrator(Administrator)
Modified	17/05/2018 15:28:23
Modification	Created as New Dataset
Parameters:	
Comments	Sample 032 By Administrator Date Thursday, May 17 2018

Figure 10. Spectrum sample history.


Login History, Audit Trail and Summary

Login History | Audit Trail | Summary

Full Name	User Name	Computer	Status	Logged In	Logged Ou
Administrator	Administrator	DESKTOP-...	OK	18 February 20...	
Administrator	Administrator	DESKTOP-...	Failed	18 February 20...	
Administrator	Administrator	DESKTOP-...	OK	30 January 20...	30 January
Analyst	Analyst	DESKTOP-...	OK	30 January 20...	30 January
Analyst	Analyst	DESKTOP-...	Failed	30 January 20...	
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Analyst	Analyst	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	25 January 20...	25 January
PEService	PEService	DESKTOP-...	OK	25 January 20...	25 January
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	
Supervisor	Supervisor	DESKTOP-...	OK	25 January 20...	25 January
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	

Login History, Audit Trail and Summary

Login History | Audit Trail | Summary

Function	Previous Value	Current Value	Full Name
Edit User Password for Administrator	Hidden	Hidden	Administrator
Edit User Password for Approver	Hidden	Hidden	Approver
Edit User Password for Supervisor	Hidden	Hidden	Supervisor
Edit User Groups for Supervisor	N/A	Reviewers	Administrator
Edit User Groups for Approver	N/A	Approvers	Administrator
Edit User Groups for Analyst	N/A	Users	Administrator
Edit User Groups for Developer	N/A	Users	Administrator
Register New Application	N/A	Spectrum ES	Administrator

Login History, Audit Trail and Summary

Login History | Audit Trail | Summary

Application: Spectrum ES

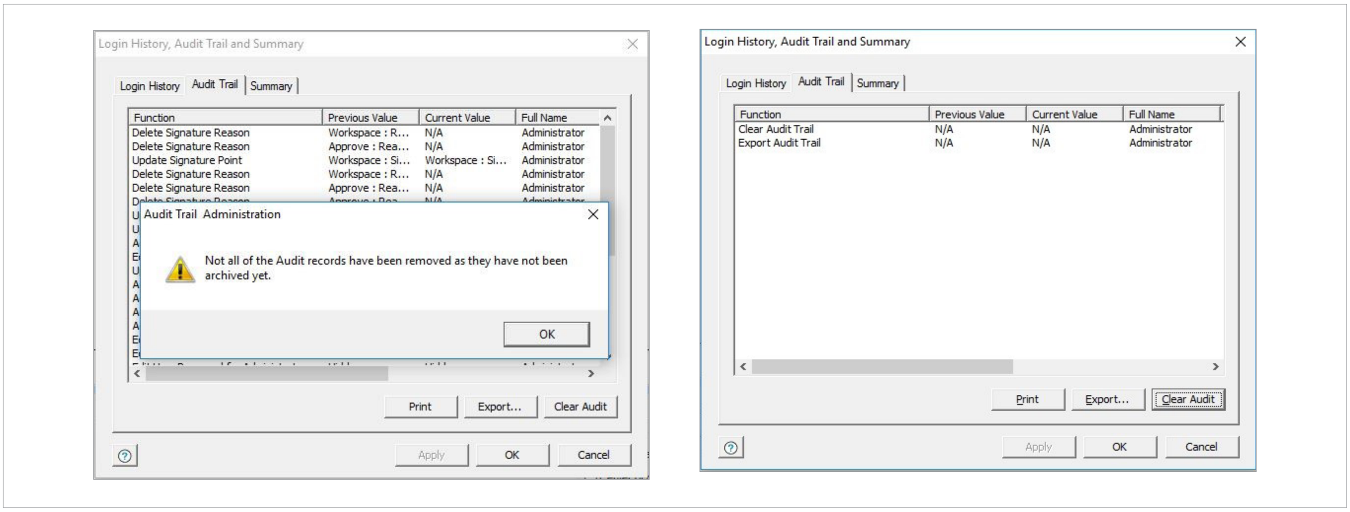
Password control:

Login Type: PerkinElmer Login
Windows Group: N/A
Maximum password age: Password expires after 42 days
Minimum password age: Allow changes after 1 days
Minimum password length: At least 6 characters
Password uniqueness: Remember the last 24 passwords
Lockout count: 5 failed logins allowed before lockout
Lockout duration: 60 minutes

Permissions: Number of Permissions = 142

Administrator [1]
Rename Sample Name [13]

Figure 11. Login history and user audit trail.



Function	Previous Value	Current Value	Full Name
Delete Signature Reason	Workspace : R...	N/A	Administrator
Delete Signature Reason	Approve : Rea...	N/A	Administrator
Update Signature Point	Workspace : Si...	Workspace : Si...	Administrator
Delete Signature Reason	Workspace : R...	N/A	Administrator
Delete Signature Reason	Approve : Rea...	N/A	Administrator

Audit Trail Administration

Not all of the Audit records have been removed as they have not been archived yet.

OK

Function	Previous Value	Current Value	Full Name
Clear Audit Trail	N/A	N/A	Administrator
Export Audit Trail	N/A	N/A	Administrator

Figure 12. Warning obtained when attempting to clear user audit trail without first exporting (left) and after exporting and clearing the audit trail (right).

An additional feature to satisfy data integrity requirements is Spectrum FL ES Report Designer. This allows a substantial amount of flexibility in generating reports and saves each report as a secured PDF. These files are encrypted in a unique PerkinElmer format so that any modification will invalidate them, preventing them from loading. Reports can only be generated in Spectrum FL ES if the appropriate permission has been applied. Similarly, Report Designer can only be opened to create or edit a template if the appropriate permissions have been applied.

Instrument Performance Testing

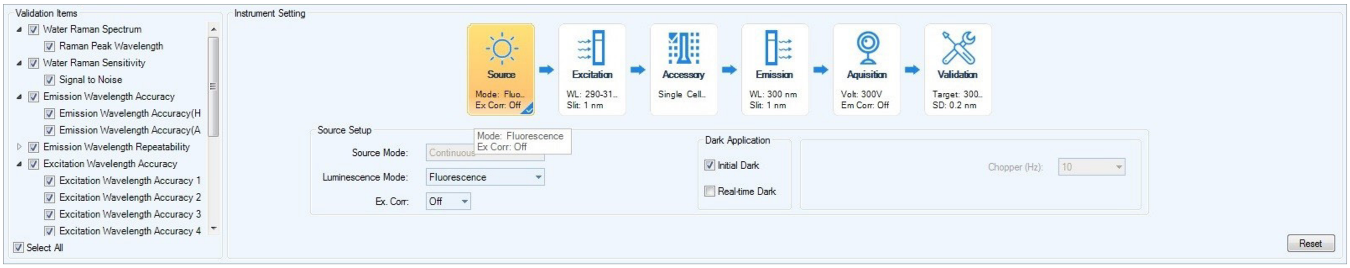
As with the standard software version, Spectrum FL ES is supplied with a validation module to enable key specifications to be tested (Figure 13). The module is very intuitive and guides the user through the process.

In addition, the PerkinElmer OneSource® UOQ program offers laboratories ongoing compliance with continuously evolving regulatory conditions.

The UOQ program includes:

- A protocol which is customizable by the user, including options to test according to pharmacopoeial requirements. When finalized, the protocol is approved and then locked so that changes are not permitted during the testing time.
- Instrument testing by a service engineer according to user defined specifications. Multiple instruments may be tested simultaneously to reduce downtime.
- The UOQ report provides an ultra-secure document including pass/fail results and built-in calculations. This report is 21 CFR Part 11 compliant.
- Digital Archiving of data making it easy to provide information required for audits.

The UOQ program supports FTIR, UV/Vis, HPLC, UPLC, and GC systems, regardless of equipment manufacturer to allow efficiencies in testing, reporting and review of annual operational qualifications.



- ☑ Water Raman Spectrum
  - ☑ Raman Peak Wavelength
- ☑ Water Raman Sensitivity
  - ☑ Signal to Noise
- ☑ Emission Wavelength Accuracy
  - ☑ Emission Wavelength Accuracy(H
  - ☑ Emission Wavelength Accuracy(A
- ☑ Emission Wavelength Repeatability
- ☑ Excitation Wavelength Accuracy
  - ☑ Excitation Wavelength Accuracy 1
  - ☑ Excitation Wavelength Accuracy 2
  - ☑ Excitation Wavelength Accuracy 3
  - ☑ Excitation Wavelength Accuracy 4

☑ Select All

Source: Mode: Fluo... Ex Corr: Off
Excitation: WL: 290-31... Slit: 1 nm
Accessory: Single Cell...
Emission: WL: 300 nm Slit: 1 nm
Aquisition: Volt: 300V Em Corr: Off
Validation: Target: 300... SD: 0.2 nm

Mode: Fluorescence
Ex Corr: Off

Source Mode: Continuous
Luminescence Mode: Fluorescence
Ex. Corr: Off

☑ Initial Dark
☐ Real-time Dark

Chopper (Hz): 10

Figure 13. Spectrum FL Validation Module.

Conclusion

PerkinElmer's Spectrum FL Enhanced Security software platform for fluorescence spectroscopy provides additional security and data integrity features for achieving compliance with 21 CFR Part 11. In addition to enhanced access control features, ES software automatically stores data, experimental parameters and audit trail information in secure databases. Data operating parameters and events can quickly and easily be recovered for inspection purposes using the "Audit Trail" feature in the ES software. Electronic signature points can be added for certain actions, defined by the system administrator, and included in the audit trail. The comprehensive instrument validation module also allows straightforward approaches to assess instrument performance.

References

1. Data Integrity and Compliance with Drug CGMP: Questions and Answers; Guidance for Industry, Food and Drug Administration, 2018.
2. The 5P Model for Data Integrity, Institute of Validation Technology, 2018. Available from: http://www.ivtnetwork.com/article/5p-model-data-integrity.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

PerkinElmer®

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs